REMARKS

Claims 1-38 are pending in this application. Claims 1, 19 and 38 are independent claims. Claims 1, 19, 27 and 38 are amended. Reconsideration and allowance of the present application are respectfully requested.

Claim Objections

Claim 27 is objected to because of informalities. Claim 27 has been amended to overcome the objection. Therefore, Applicants respectfully request that the objection to claim 27 be withdrawn.

Claim Rejections under 35 U.S.C. §101

Claim 38 stands rejected under 35 U.S.C. §101 as allegedly being directed to non-statutory subject matter. Claim 38 has been amended to overcome the rejection. Therefore, Applicants respectfully request that the rejection of claim 38 under 35 U.S.C. §101 be withdrawn.

Claim Rejections under 35 U.S.C. §102

Claims 1-38 stand rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,587,945 to Pasieka (hereinafter "Pasieka"). This rejection is respectfully traversed.

As outlined below, Pasieka does not teach or suggest each of the elements recited in claims 1-38.

Pasieka discloses that an author uses an imager to create an image and the image is automatically sent to a server which signs and stores the image. In particular, the author operates an imager to create an image and initiates submitting the image to a secure server. The imager transmits the image to a secure server over a secure channel. Preferably, the transmission will identify the author and the imager device. The server may return an image sequence number for the imager to facilitate later access to the image. The server combines the imager ID (or author ID) and image sequence number with the image to produce an image record and stores the image record. The server hashes the image record using a one-way hash to produce an image

fingerprint. A hash of a digital document is commonly referred to as a digital fingerprint. The server encrypts the image fingerprint using the server's private key (or author's or imager's private keys stored in the server) to form an image signature. The purpose of the encryption is to provide proof that the author is the originator of the image, and that the image has not been altered by others since it was signed. The encryption of the hash has nothing to do with keeping the data or the hash secret but only to prove integrity and origin of the image. See at least Col. 4 of Pasieka.

Applicants submit that Pasieka does not teach or suggest each of the elements recited in claims 1-38. Independent claim 1, in part, recites "a memory configured to store electronic image data corresponding to an original document having an electronic, displayable verifiable provenance, and separately derived electronic displayable verification information corresponding to the provenance of at least part of the original document."

Independent claim 19, in part, recites "creating electronic image data corresponding to an original document having an electronic, displayable verifiable provenance" and "providing electronic, displayable verification information corresponding to the provenance of at least part of the original document."

Independent claim 38, in part, recites "wherein the electronic signal comprises electronic image data corresponding to an original document having an electronic, displayable verifiable provenance, and electronic, displayable verification information corresponding to the provenance of at least part of the original document." Pasieka does not teach or suggest these features.

Pasieka fails to teach or suggest that the original document includes an electronic, displayable verifiable provenance. In Pasieka, the origin and integrity of the image is proven by the image signature. The image signature in Pasieka is formed by combining the imager ID and image sequence number with the image to produce an image record which the server uses with a one-way hash to produce an image fingerprint. The server then encrypts the image fingerprint using a private key to form the image signature. The image signature of Pasieka does not correspond to the "electronic displayable verification information corresponding to the provenance of at least part of the original document." Rather, the image signature of Pasieka corresponds to an image fingerprint created by the server for the entire document.

Therefore, Pasieka does not teach or suggest "an original document having an electronic, displayable verifiable provenance, and separately derived electronic displayable verification information corresponding to the provenance of at least part of the original document," as recited in claims 1, 19 and 38. Each of claims 2-18 and 20-37 depends on and incorporates all of the elements of claims 1 and 19, in addition to the further elements recited in claims 2-18 and 20-37. Therefore, Applicants respectfully request that this rejection of claims 1-38 under 35 U.S.C. §102 be withdrawn.

Disclaimer

Applicants may not have presented all possible arguments or have refuted the characterizations of either the claims or the prior art as found in the Office Action. However, the lack of such arguments or refutations is not intended to act as a waiver of such arguments or as concurrence with such characterizations.

CONCLUSION

In view of the above, consideration and allowance are respectfully solicited.

In the event the Examiner believes an interview might serve in any way to advance the prosecution of this application, the undersigned is available at the telephone number noted below.

The Office is authorized to charge any necessary fees to Deposit Account No. 22-0185.

Applicant believes no fee is due with this response. However, if a fee is due, please charge our Deposit Account No. 22-0185, under Order No. 27592-01057-US3 from which the undersigned is authorized to draw.

Dated: January 8, 2009

Respectfully submitted,

Electronic signature: /Arlene P. Neal/
Arlene P. Neal
Registration No.: 43,828
CONNOLLY BOVE LODGE & HUTZ LLP
1875 Eye Street, NW
Suite 1100
Washington, DC 20006
(202) 331-7111
(202) 293-6229 (Fax)
Attorney for Applicant